Bug 721940 (CVE-2019-19721, VideoLAN-SB-VLC-309) - <media-video/vlc-3.0.10: out of bound read (VideoLAN-SB-VLC-309)

Status: RESOLVED FIXED
Alias: CVE-2019-19721, VideoLAN-SB-VLC-309
Product: Gentoo Security
Component: Vulnerabilities (show other bugs)
Hardware: All Linux
Importance: Normal normal
Assignee: Gentoo Security
URL: https://www.videolan.org/security/sb-...
Whiteboard: B2 [glsa+ cve cleanup]
Keywords: CC-ARCHES
Depends on:
Blocks:

Reported: 2020-05-09 18:22 UTC by GLSAMaker/CVETool Bot
Modified: 2020-05-14 22:27 UTC (History)
CC List: 1 user (show)
See Also: ~~CVE-2020-6071, CVE-2020-6072, CVE-2020-6073, CVE-2020-6077, CVE-2020-6078, CVE-2020-6079, CVE-2020-6080~~
Flags: nattka: sanity-check+

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Note: Please do not mark this bug as resolved after bumping or stabilizing. The Security Team will take care of that. Thanks.

GLSAMaker/CVETool Bot Dev **2020-05-09 18:22:15 UTC** Description

```
Incoming details.
```

Thomas Deutschmann (RETIRED) Dev **2020-05-09 18:25:18 UTC** Comment 1

```
From $URL:

Details
=======
A remote user could:

- Create a specifically crafted image file that could trigger an out of bounds read

If successful, a malicious third party could trigger either a crash of VLC or an
arbitratry code execution with the privileges of the target user.

While these issues in themselves are most likely to just crash the player, we can't
exclude that they could be combined to leak user informations or remotely execute
code. ASLR and DEP help reduce the likelyness of code execution, but may be
```

bypassed.

We have not seen exploits performing code execution through these vulnerabilities

CVE-2019-19721 affects VLC 3.0.8 and earlier, and only reads 1 byte out of bound
Threat mitigation

Exploitation of those issues requires the user to explicitly open a specially crafted file or stream.

Workarounds
==========
The user should refrain from opening files from untrusted third parties or accessing untrusted remote sites (or disable the VLC browser plugins), until the patch is applied.

Sergei Trofimovich (RETIRED) Dev **2020-05-09 23:18:59 UTC** Comment 2

ppc/ppc64 stable

Agostino Sarubbo Dev **2020-05-11 11:29:26 UTC** Comment 3

amd64 stable

Agostino Sarubbo Dev **2020-05-12 06:40:35 UTC** Comment 4

x86 stable

Sam James AT InFra Dev Sec **2020-05-12 16:10:23 UTC** Comment 5

arm64 stable.

@maintainer(s), please cleanup

Sam James AT InFra Dev Sec **2020-05-13 00:29:53 UTC** Comment 6

Note that the microdns issues were handled in ~~bug 714606~~.

For this bug, we have:
https://git.videolan.org/?p=vlc/vlc-3.0.git;a=commit;h=72afe7ebd8305bf4f5360293b8621cde52ec506b

GLSAMaker/CVETool Bot Dev **2020-05-14 22:25:58 UTC** Comment 7

This issue was resolved and addressed in
 GLSA 202005-11 at https://security.gentoo.org/glsa/202005-11
by GLSA coordinator Thomas Deutschmann (whissi).

Larry the Git Cow Dev **2020-05-14 22:27:24 UTC** Comment 8

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=a4ebc3f825cadf3aafc60e70aec4f5952ebe8853

commit a4ebc3f825cadf3aafc60e70aec4f5952ebe8853
Author: Thomas Deutschmann <whissi@gentoo.org>

```
AuthorDate: 2020-05-14 22:27:09 +0000
Commit:     Thomas Deutschmann <whissi@gentoo.org>
CommitDate: 2020-05-14 22:27:16 +0000

    media-video/vlc: security cleanup

    Bug: https://bugs.gentoo.org/721940
    Package-Manager: Portage-2.3.99, Repoman-2.3.22
    Signed-off-by: Thomas Deutschmann <whissi@gentoo.org>

 media-video/vlc/Manifest            |   1 -
 media-video/vlc/vlc-3.0.8-r1.ebuild | 489 ------------------------------------
 2 files changed, 490 deletions(-)
```

Format For Printing - XML - Clone This Bug - Clone In The Same Product - Top of page